(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 41 38 861 A 1**

(51) Int. Cl.[5]:
H 04 L 9/32
G 06 F 12/14
G 07 C 9/00
G 07 F 7/12

(21) Aktenzeichen: P 41 38 861.5
(22) Anmeldetag: 26. 11. 91
(43) Offenlegungstag: 1. 10. 92

DE 41 38 861 A 1

Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

(71) Anmelder:
Siemens Nixdorf Informationssysteme AG, 4790 Paderborn, DE

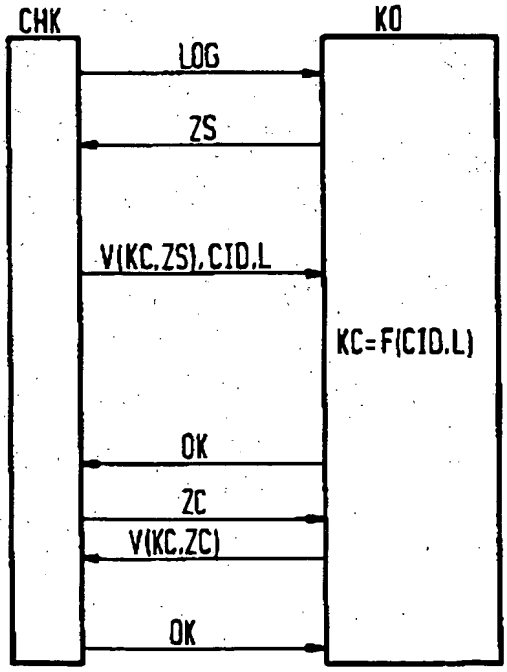
(74) Vertreter:
Fuchs, F., Dr.-Ing., Pat.-Anw., 8000 München

(72) Erfinder:
Laschinger, Bertold, Dr., 8011 Aying, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners mit einem Kommunikationssystem

(57) Eine mögliche Manipulation an einem Kommunikationssystem (KO), die sich aus der Verwendung einer Chipkartenidentitätskenngröße (CID) für mehrere Chipkarten (CHK) ergibt, wird wirksam dadurch verhindert, daß jeder Chipkarte (CHK) zusätzlich zur Chipkartenidentitätskenngröße (CID) eine Zusatzidentitätskenngröße (L) zugeordnet wird. Ein chipkartenspezifischer Schlüssel (KC) wird mit Hilfe der beiden Kenngrößen erzeugt.



DE 41 38 861 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners nach der "Challenge and Response" Methode mit einem Kommunikationssystem gemäß dem Oberbegriff des Anspruchs 1.

Um Zugang zu einem Kommunikationssystem zu erhalten, muß häufig die Berechtigung zu diesem Zugang nachgewiesen werden. Andererseits muß sich auch das Kommunikationssystem eindeutig als echt zu erkennen geben, um einen möglichen Betrug durch ein simuliertes Kommunikationssystem auszuschließen. Um dies zu gewährleisten, wurde die sogenannten "Challenge and Response" Methode entwickelt.

Bei dieser Methode schickt zunächst das Kommunikationssystem eine Zufallszahl an den elektronischen Partner. Dieser verschlüsselt diese Zufallszahl mit einem Verschlüsselungsalgorithmus und einem Schlüssel und sendet das Ergebnis gemeinsam mit einer Identitätskenngröße zurück an das Kommunikationssystem. Mittels eines nur dem Kommunikationssystem bekannten Verfahrens errechnet das Kommunikationssystem aus der Identitätskenngröße den Schlüssel und errechnet ebenfalls das Ergebnis, das sich mit Hilfe des Verschlüsselungsalgorithmus aus der Zufallszahl und dem Schlüssel ergibt. Stimmt das vom elektronischen Partner gesendete Ergebnis mit dem vom Kommunikationssystem errechneten überein, gilt der elektronische Partner als authentisch.

Zur Authentisierung des Kommunikationssystems gegenüber dem elektronischen Partner wird der oben beschriebene Vorgang mit vertauschten Rollen nochmals durchgeführt. Der elektronische Partner sendet eine Zufallszahl zum Kommunikationssystem, das Kommunikationssystem verschlüsselt diese Zufallszahl anhand des Verschlüsselungsalgorithmus und des ihm bereits bekannten Schlüssels und sendet das Ergebnis zum Vergleich an den elektronischen Partner.

Der Schlüssel ist demnach lediglich im elektronischen Partner gespeichert, während das Kommunikationssystem diesen Schlüssel immer wieder neu nach einem nur dem Kommunikationssystem bekannten Verfahren unter Zugrundelegen der Identitätskenngröße des elektronischen Partners erzeugen muß. Diese Identitätskenngröße wird während der Initialisierungsphase, d. h. vor dem erstmaligen Betrieb des Kommunikationssystems gemeinsam mit den elektronischen Partnern, für die elektronischen Partner festgelegt. Dabei erscheint es häufig sinnvoll, ganzen Gruppen von elektronischen Partnern die gleiche Identitätskenngröße und damit auch den gleichen Schlüssel zuzuordnen.

Auf Grund dieser Praxis ergibt sich aber für einen Betrüger die Möglichkeit, das Kommunikationssystem gegenüber einem elektronischen Partner zu simulieren. Voraussetzung ist lediglich, daß zwei elektronische Partner mit gleicher Identitätskenngröße annähernd gleichzeitig auf das Kommunikationssystem zugreifen wollen. Diese Simulation des Kommunikationssystems kann dann auf folgende Weise durchgeführt werden:

Das simulierte Kommunikationssystem sendet eine Zufallszahl zum ersten elektronischen Partner, dieser verschlüsselt die Zufallszahl in oben beschriebener Weise und sendet das Ergebnis gemeinsam mit der Identitätskenngröße zum simulierten Kommunikationssystem. Dieses bestätigt die Richtigkeit des Ergebnisses, ohne es wirklich überprüft zu haben, woraufhin der erste elektronische Partner eine weitere Zufallszahl zum simulierten Kommunikationssystem sendet. Dieses reicht die soeben empfangene Zufallszahl zum zweiten elektronischen Partner weiter, der daraus in oben beschriebener Weise das benötigte Verschlüssellungsergebnis berechnet und es an das simulierte Kommunikationssystem überträgt. Das simulierte Kommunikationssystem reicht dieses Ergebnis zum ersten elektronischen Partner weiter, der es mit dem selbst errechneten Ergebnis vergleicht und die Authentizität des simulierten Kommunikationssystems feststellt. Der zweite elektronische Partner wird durch Übertragung einer Fehlermeldung vom simulierten Kommunikationssystem abgewiesen.

Die der vorliegenden Erfindung zugrundeliegende Aufgabe ist es nun, bei mehrfacher Verwendung einer Identitätskenngröße für mehrere elektronische Partner, die gleichzeitig an ein Kommunikationssystem angeschlossen sein können, eine Simulation des Kommunikationssystems in betrügerischer Absicht zu verhindern.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

Durch das Hinzufügen der Zusatzidentitätskenngröße zur Identitätskenngröße kann in vorteilhafter Weise für jeden elektronischen Partner ein individueller Schlüssel errechnet werden. Damit kann im Falle der Zusammenfassung von elektronischen Partnern in Gruppen mit identischen Identitätskenngrößen einer betrügerischen Simulation des Kommunikationssystems gegenüber einem elektronischen Partner erfolgreich begegnet werden.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung, sowie eine vorteilhafte Verwendung, sind in den Unteransprüchen angegeben.

Im folgenden wird die Erfindung anhand der Zeichnung näher erläutert. Dabei zeigen

Fig. 1 den Verfahrensablauf bei simuliertem Kommunikationssystem und

Fig. 2 den erfindungsgemaßen Verfahrensablauf.

Im folgenden wird anstelle des Begriffes "elektronischer Partner", der für ein beliebig ausgeformtes elektronisches Gerät mit den Fähigkeiten einer Chipkarte steht, der Begriff "Chipkarte" verwendet.

Am linken Rand der Fig. 1 ist symbolisch eine erste Chipkarte CHK1 und am rechten Rand symbolisch eine zweite Chipkarte CHK2 gezeigt. Zwischen den beiden Chipkarten CHK1, CHK2 ist symbolisiert durch ein Rechteck ein simuliertes Kommunikationssystem SKO abgebildet. Zu einem bestimmten Zeitpunkt wird beispielsweise durch Einstecken der ersten Chipkarte CHK1 in ein Kartenlesegerät die erste Chipkarte CHK1 mit dem simulierten Kommunikationssystem SKO verbunden. Die erste Chipkarte CHK1 überträgt an das simulierte Kommunikationssystem SKO eine AnmeldeInformation LOG. Daraufhin überträgt das simulierte Kommunikationssystem SKO eine erste Zufallszahl ZB zur ersten Chipkarte CHK1. Diese verschlüsselt anhand des Verschlüsselungsalgorithmus V und des in der Karte gespeicherten Schlüssels K die erste Zufallszahl ZB. Das Verschlüsselungsergebnis V (K, ZB) und die in der ersten Chipkarte CHK1 gespeicherte Chipkartenidentitätsnummer CID werden zum simulierten Kommunikationssystem SKO übertragen. Das simulierte Kommunikationssystem SKO überträgt ein Quittungssignal OK an die erste Chipkarte CHK1. Die erste Chipkarte CHK1 interpretiert das Quittungssignal OK so, als wäre der Authentifizierungsprozeß der ersten Chipkare CHK1 gegenüber dem simulierten Kommunikationssystem SKO erfolgreich verlaufen. Deshalb sendet die er-

ste Chipkarte CHK1 zur Authentizitätsprüfung des simulierten Kommunikationssystems SKO eine zweite Zufallszahl ZC zum simulierten Kommunikationssystem SKO.

Wird nun gleichzeitig oder annähernd gleichzeitig eine zweite Chipkarte CHK2, beispielsweise durch Einschieben in ein weiteres Kartenlesegerät mit dem simulierten Kommunikationssystem SKO verbunden, so ergibt sich für den Fall, daß die zweite Chipkarte CHK2 die gleiche Chipkartenidentitätsnummer CID wie die erste Chipkarte CHK1 trägt, folgende Situation: Zunächst meldet sich auch die zweite Chipkarte CHK2 durch Übertragen einer Anmeldeinformation LOG beim simulierten Kommunikationssystem SKO an. Das simulierte Kommunikationssystem SKO reicht nun die von der ersten Chipkarte CHK1 empfangene zweite Zufallszahl ZC an die zweite Chipkarte CHK2 weiter. Die zweite Chipkarte CHK2 verschlüsselt diese zweite Zufallszahl ZC mit Hilfe des Verschlüsselungsalgorithmus V und des Schlüssels K und gibt das Verschlüsselungsergebnis V (K, ZC) und die Kartenidentitätsnummer CID zum simulierten Kommunikationssystem SKO. Das simulierte Kommunikationssystem SKO verfügt nun über das zur Authentifikation gegenüber der ersten Chipkarte CHK1 erforderliche Verschlüsselungsergebnis V (K, ZC) und überträgt dieses zur ersten Chipkarte CHK1. Die gegenseitige Authentifikation zwischen erster Chipkarte CHK1 und simuliertem Kommunikationssystem SKO ist damit erfolgreich abgeschlossen. Die zweite Chipkarte CHK2 erhält ein negatives Quittungssignal F und wird damit abgewiesen.

In **Fig.** 2 ist nun aufgezeigt, wie die oben beschriebene Authentifikation eines simulierten und damit unberechtigten Kommunikationssystems SKO gegenüber einer Chipkarte CHK wirksam verhindert werden kann. Während des Initialisierungsprozesses, der vor der ersten Inbetriebnahme einer mit Hilfe von Chipkarten realisierbaren Anwendung in einem Kommunikationssystem KO abläuft, wird vom zukünftigen Benutzer der Chipkarten CHK die Chipkartenidentitätskenngröße CID festgelegt. Beispielsweise kann die Chipkartenidentitätskenngröße CID der Name oder die Nummer einer Abteilung innerhalb eines Betriebes sein. Zusätzlich zu dieser Chipkartenidentitätskenngröße CID wird während des Initialisierungsprozesses für jede Chipkarte eine Zufallszahl generiert, die der jeweiligen Chipkarte CHK als Zusatzidentitätsgröße L zugeordnet wird. Nach einer festzulegenden Funktion wird aus den Parametern Chipkartenidentitätskenngröße CID und der Zusatzidentitätskenngröße L ein chipkartenspezifischer Schlüssel KC erzeugt. Dieser spezifische Schlüssel KC, die Chipkartenidentitätskenngröße CID und die Zusatzidentitätskenngröße L werden in der Chipkarte CHK gespeichert. Im Kommunikationssystem KO wird lediglich vermerkt, welches Verfahren zur Errechnung des Schlüssels KC aus der Chipkartenidentitätskenngröße CID und der Zusatzidentitätskenngröße L bei der jeweiligen Anwendung Verwendung finden soll.

Die gegenseitige Authentifikation zwischen Chipkarte CHK und Kommunikationssystem KO verläuft dann wie folgt: Die Chipkarte CHK überträgt eine Anmeldeinformation LOG an das Kommunikationssystem KO. Das Kommunikationssystem KO erzeugt eine Zufallszahl ZS und überträgt diese zur Chipkarte CHK. Die Chipkarte errechnet aus dem spezifischen Schlüssel KC und der Zufallszahl ZS ein Verschlüsselungsergebnis V (KC, ZS) und überträgt dieses gemeinsam mit der Chipkartenidentitätskenngröße CID und der Zusatzidentitätskenngröße L zum Kommunikationssystem KO. Das Kommunikationssystem KO errechnet aus der Chipkartenidentitätskenngröße CID und der Zusatzidentitätskenngröße L mit Hilfe des festgelegten Verfahrens F den spezifischen Schlüssel KC. Das Kommunikationssystem KO berechnet ebenfalls das Verschlüsselungsergebnis V (KC, ZS) und vergleicht es mit dem in der Chipkarte errechneten und zum Kommunikationssystem übertragenen Verschlüsselungsergebnis V (KC, ZS). Bei positivem Vergleichsergebnis überträgt das Kommunikationssystem KO ein positives Quittungssignal OK an die Chipkarte CHK. Diese überträgt daraufhin eine weitere Zufallszahl ZG zum Kommunikationssystem KO, wo diese verschlüsselt wird und das Verschlüsselungsergebnis V (KC, ZC) zur Chipkarte CHK übertragen und dort überprüft wird. Bei positivem Vergleichsergebnis sendet die Chipkarte CHK ein positives Quittungssignal OK zum Kommunikationssystem KO. Die gewünschte Anwendung ist damit freigegeben.

Patentansprüche

1. Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners nach der "Challenge and Response" Methode mit einem Kommunikationssystem, auf das eine Vielzahl von elektronischen Partnern zugreifen darf, von denen jeweils mehrere gleichberechtigt in Gruppen mit gleicher Identitätskenngröße zusammengefaßt sind, **dadurch gekennzeichnet**, daß jedem der gleichberechtigten elektronischen Partner (CHK) jeweils eine individuelle Zusatzidentitätskenngröße (L) zugeordnet wird, und daß diese Zusatzidentitätskenngröße (L) gemeinsam mit der Identitätskenngröße (CID) im Kommunikationssystem (KO) zur Erzeugung eines individuellen Schlüssels (KC) verwendet wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Zusatzidentitätskenngröße (L) durch einen Zufallsgenerator erzeugt wird.
3. Verwendung des Verfahrens nach einem der vorhergehenden Ansprüche in einem Kommunikationssystem, mit dem Chipkarten als elektronische Partner (CHK) kommunizieren.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 41 38 861 A1
Int. Cl.[5]: H 04 L 9/32
Offenlegungstag: 1. Oktober 1992

FIG1

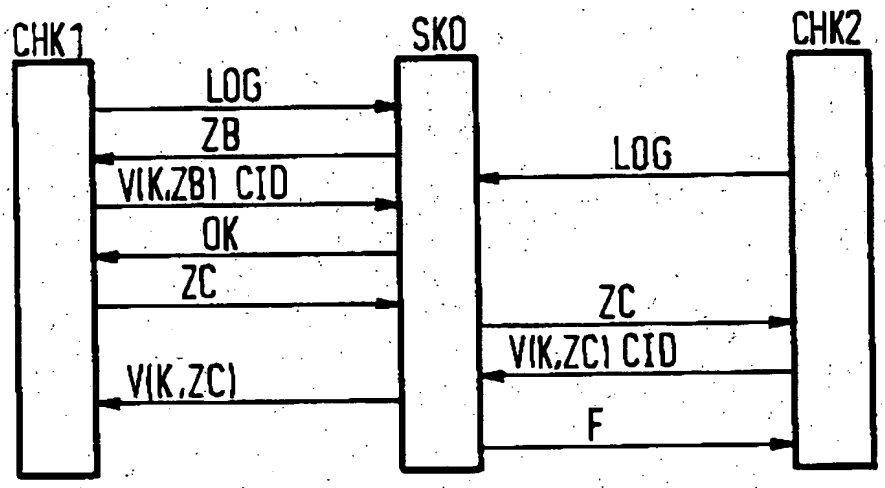


FIG2